

FIG. 1

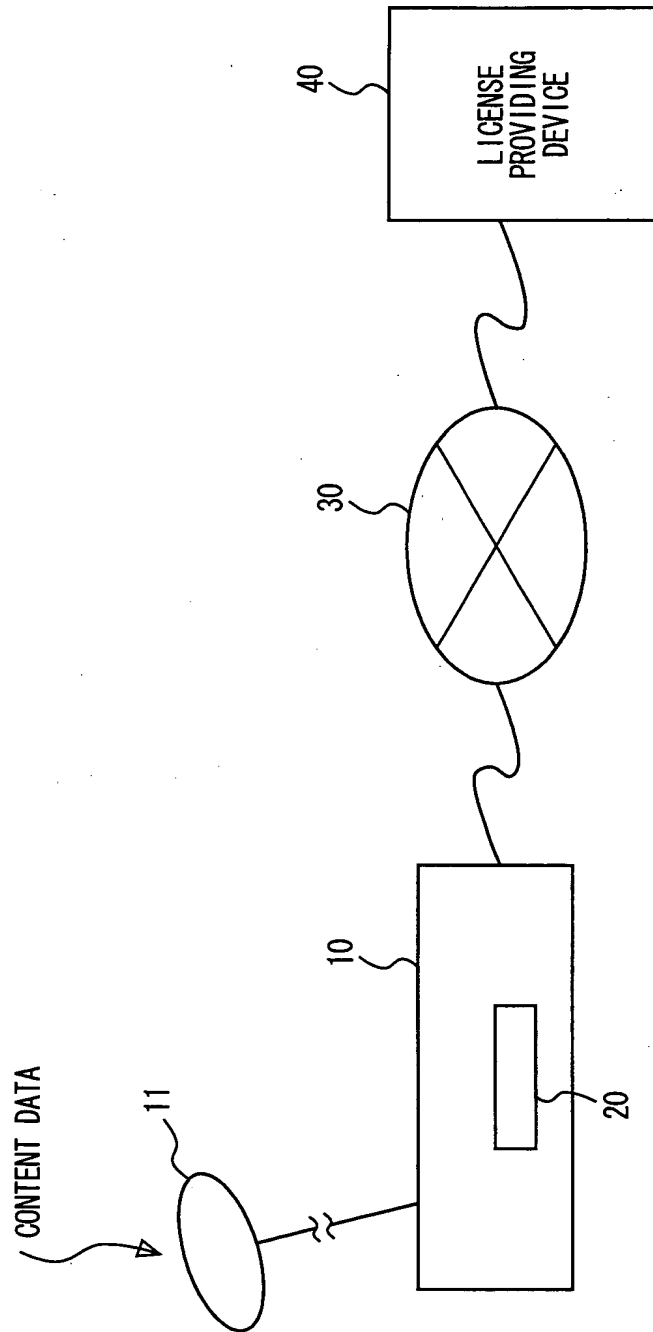


FIG. 2

SYMBOL	NAME	ATTRIBUTE	CHARACTERISTICS
Dc	DATA	PECULIAR TO DATA	EX.: MUSIC, READING, EDUCATIONAL OR IMAGE DATA, RECORDED AND MANAGED AS ENCRYPTED CONTENT DATA E(Kc, Dc) ENCRYPTED WITH Kc
Di	DATA INFORMATION	PECULIAR TO DATA	PLAINTEXT DATA RELATED TO Dc AND INCLUDING DID
DID	DATA ID	PECULIAR TO DATA	MANAGEMENT CODE FOR SPECIFYING Dc AND Kc
Kc	CONTENT KEY	PECULIAR TO DATA	SYMMETRIC KEY ENCRYPTING/DECRYPTING ENCRYPTED DATA
AC	CONTROL INFORMATION	PECULIAR TO LICENSE	RESTRICTIONS RELATED TO REPRODUCTION AND LICENSE HANDLING
LID	LICENSE ID	PECULIAR TO LICENSE	MANAGEMENT CODE FOR SPECIFYING LICENSE
LIC	LICENSE	PECULIAR TO LICENSE	GENERALLY REPRESENTING Kc//AC//DID//LID

FIG. 3

	SYMBOL	NAME	CHARACTERISTIC
LICENSE PROVIDING DEVICE	KPa	CERTIFICATION KEY	PUBLIC DECRYPTION KEY FOR VERIFYING CERTIFICATE BY CERTIFICATION AUTHORITY OPERATED BY LICENSE PROVIDER SIDE
	Ks1x	SESSION KEY	TEMPORARY KEY PRODUCED FOR EVERY LICENSE DISTRIBUTION SYMMETRIC KEY
	Ka	MASTER KEY	PRIVATE ENCRYPTION KEY TO BE USED FOR PRODUCING CLASS CERTIFICATE OPERATED BY CERTIFICATION AUTHORITY
DATA STORAGE DEVICE (HARD DISK)	KPa	CERTIFICATION KEY	PUBLIC DECRYPTION KEY FOR VERIFYING CERTIFICATE BY CERTIFICATION AUTHORITY OPERATED BY LICENSE PROVIDER SIDE
	KPomy	CLASS PUBLIC KEY	ENCRYPTION KEY ASSIGNED TO CLASS (UNIT SUCH AS TYPE) OF DEVICE "y" IS IDENTIFIER IDENTIFYING CLASS
	Komy	CLASS PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH CLASS PUBLIC KEY KPomy
	lomy	CLASS INFORMATION	INFORMATION DATA OF DEVICE AND CLASS PUBLIC KEY IN EACH CLASS
	Gmy	CLASS CERTIFICATE	$Gmy = KPomy // lomy // E(Ka, H(KPomy // lomy))$ CORRECTNESS IS VERIFIED WITH CERTIFICATION KEY KPa
	KPomz	INDIVIDUAL PUBLIC KEY	INDIVIDUAL PUBLIC ENCRYPTION KEY HAVING VALUE PECULIAR TO EACH DATA STORAGE DEVICE "z" IS IDENTIFIER IDENTIFYING DATA STORAGE DEVICE
	Komz	INDIVIDUAL PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH INDIVIDUAL PUBLIC KEY KPomz
	Ks1x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE PROVIDER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY
	Ks2x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE RECEIVER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY
	KPcpy	CLASS PUBLIC KEY	ENCRYPTION KEY ASSIGNED TO CLASS (UNIT SUCH AS TYPE) OF DEVICE "y" IS IDENTIFIER IDENTIFYING CLASS
REPRODUCING CIRCUIT	Kcpy	CLASS PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH CLASS PUBLIC KEY KPcpy
	lcpy	CLASS INFORMATION	INFORMATION DATA OF DEVICE AND CLASS PUBLIC KEY IN EACH CLASS
	Gpy	CLASS CERTIFICATE	$Gpy = KPcpy // lcpy // E(Ka, H(KPcpy // lcpy))$ CORRECTNESS IS VERIFIED WITH CERTIFICATION KEY KPa
	Ks2x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE RECEIVER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY

FIG. 4

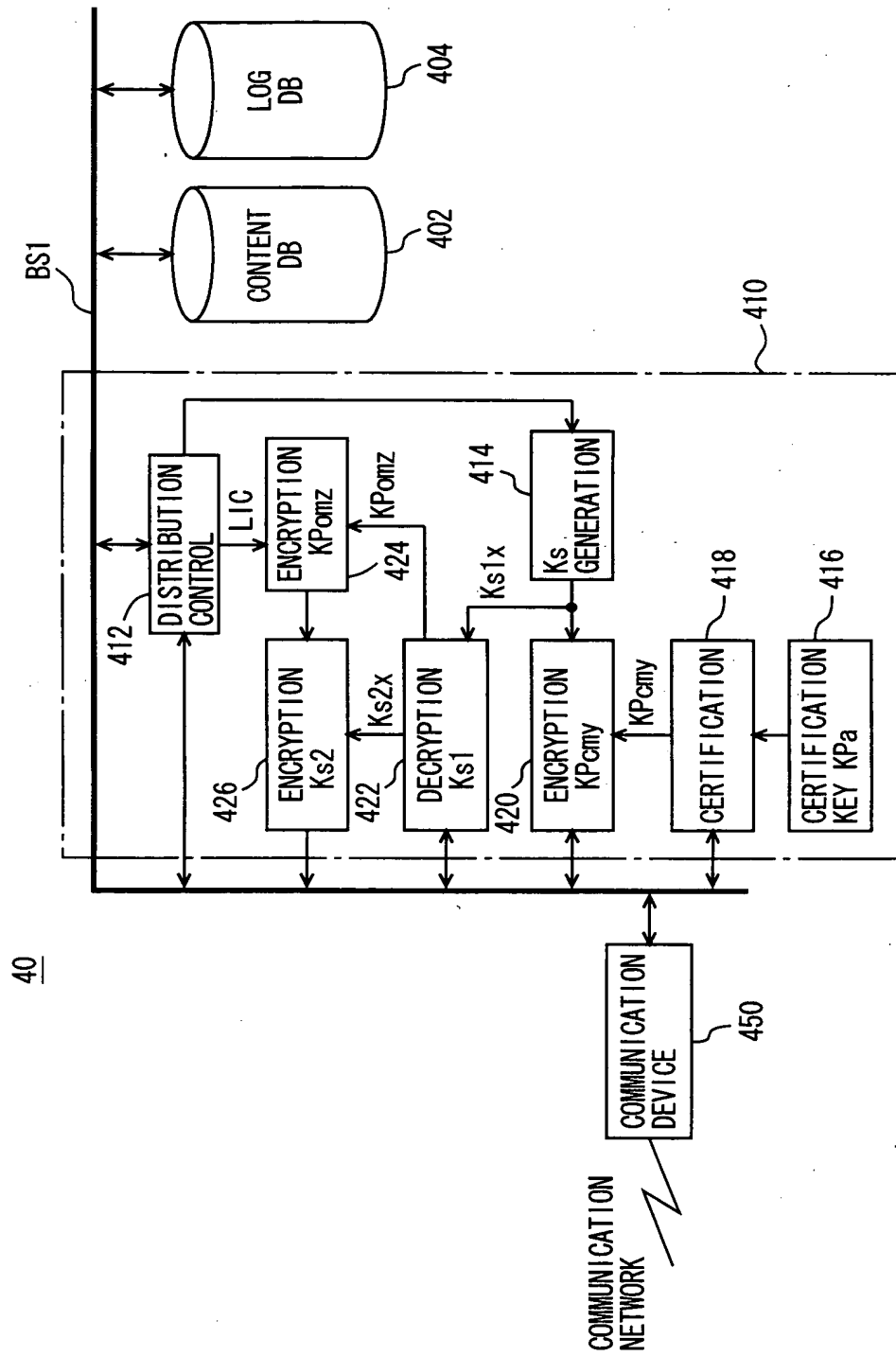


FIG. 5

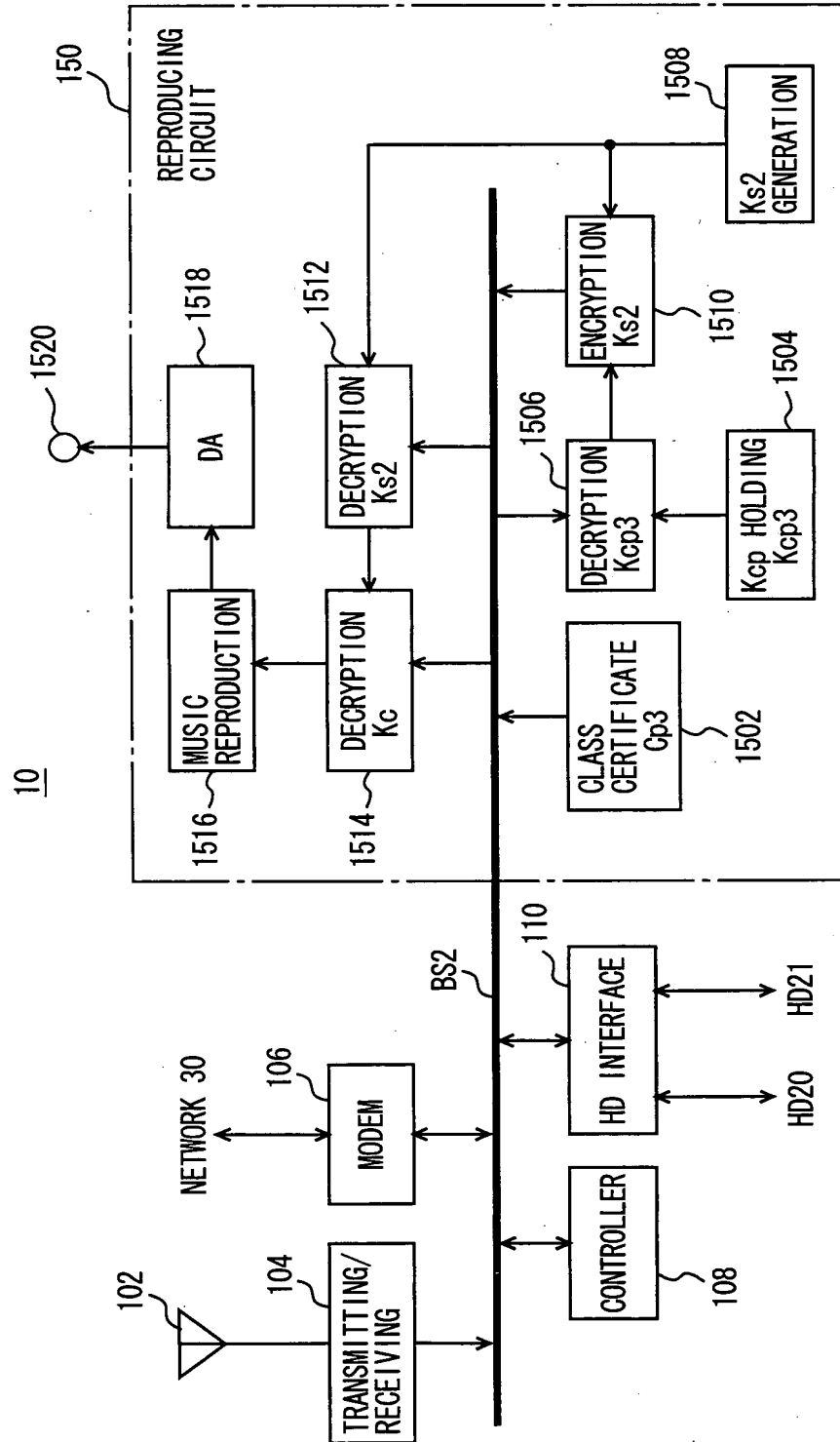


FIG. 6

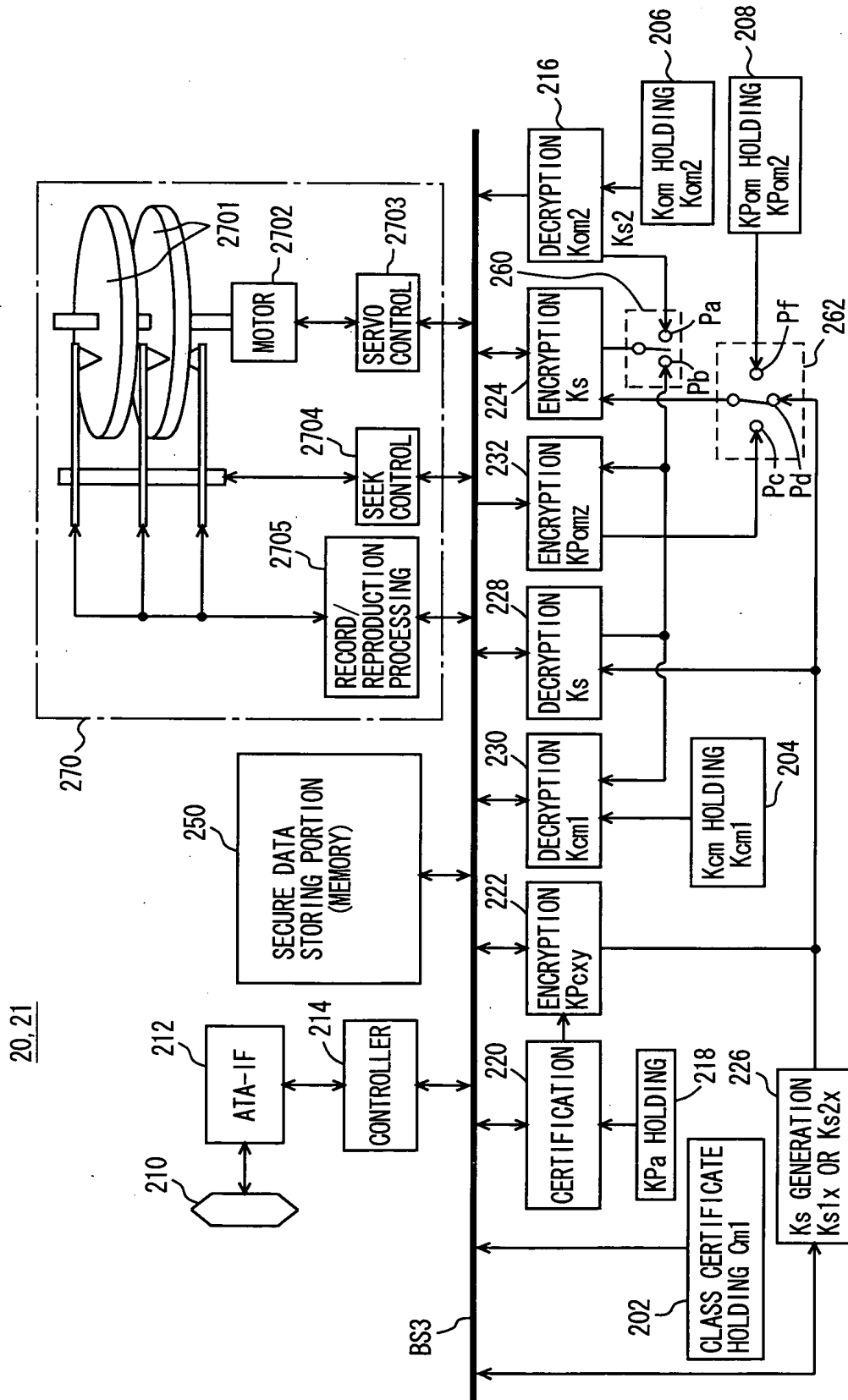


FIG. 7

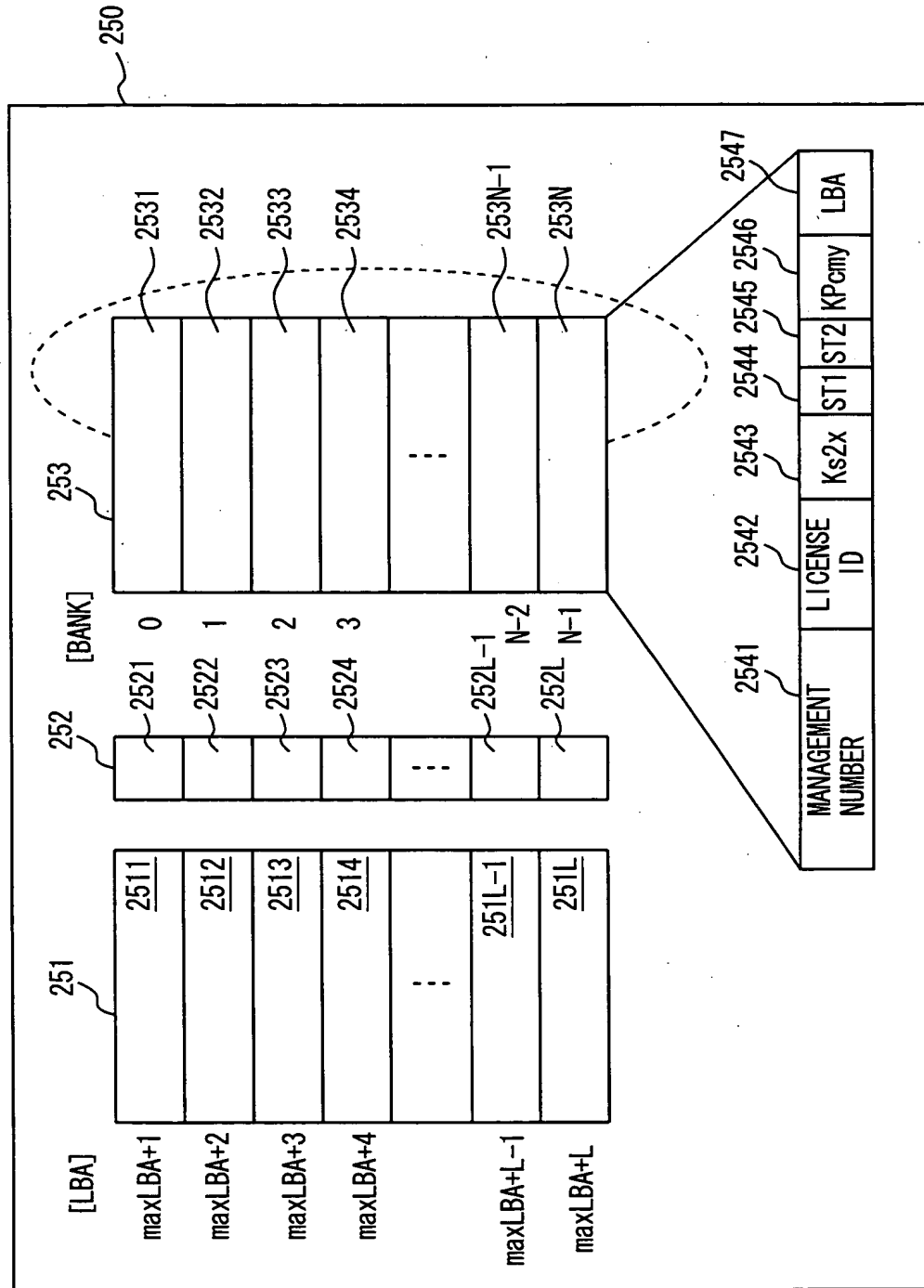


FIG. 8

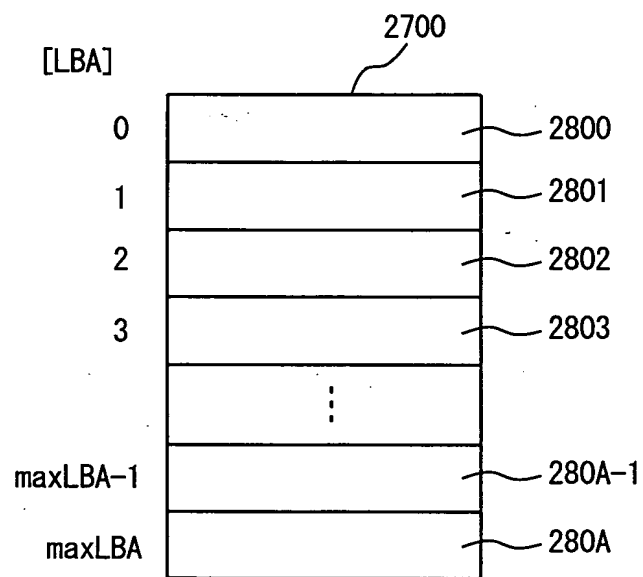


FIG. 9

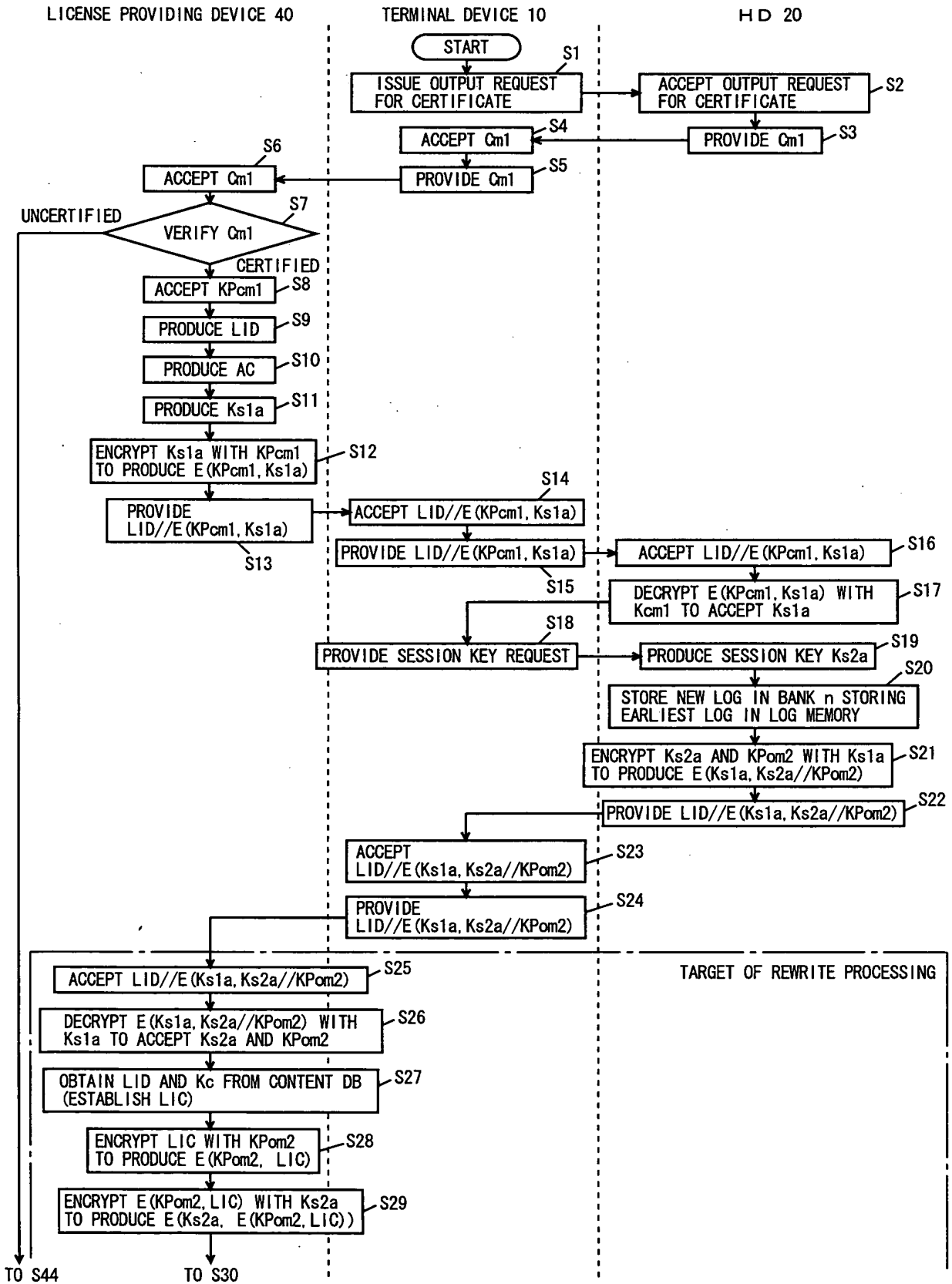


FIG. 10

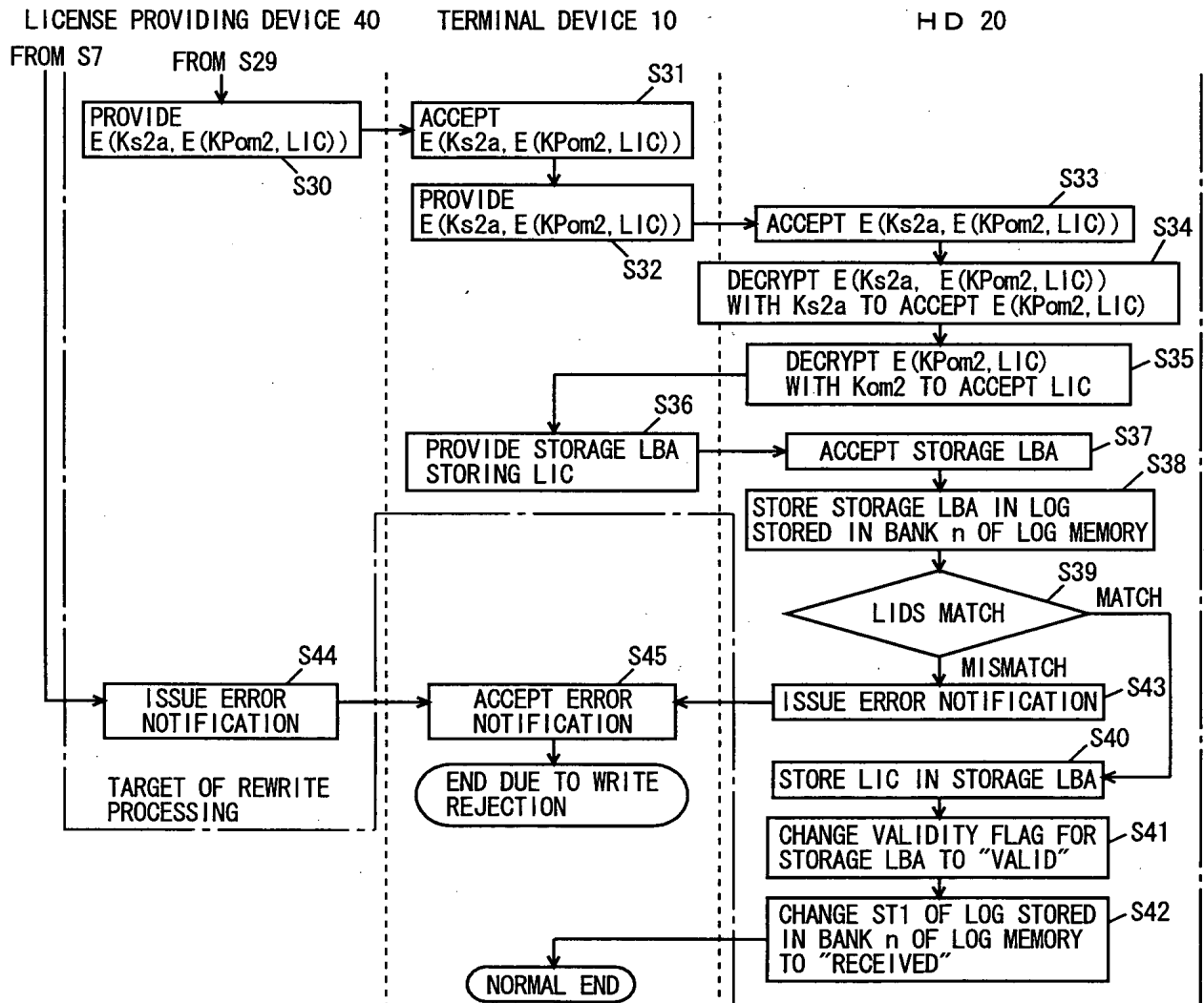


FIG. 11

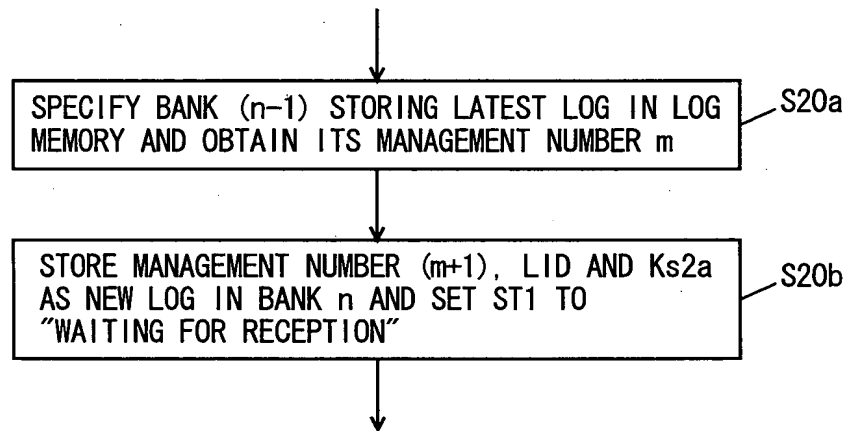


FIG. 12

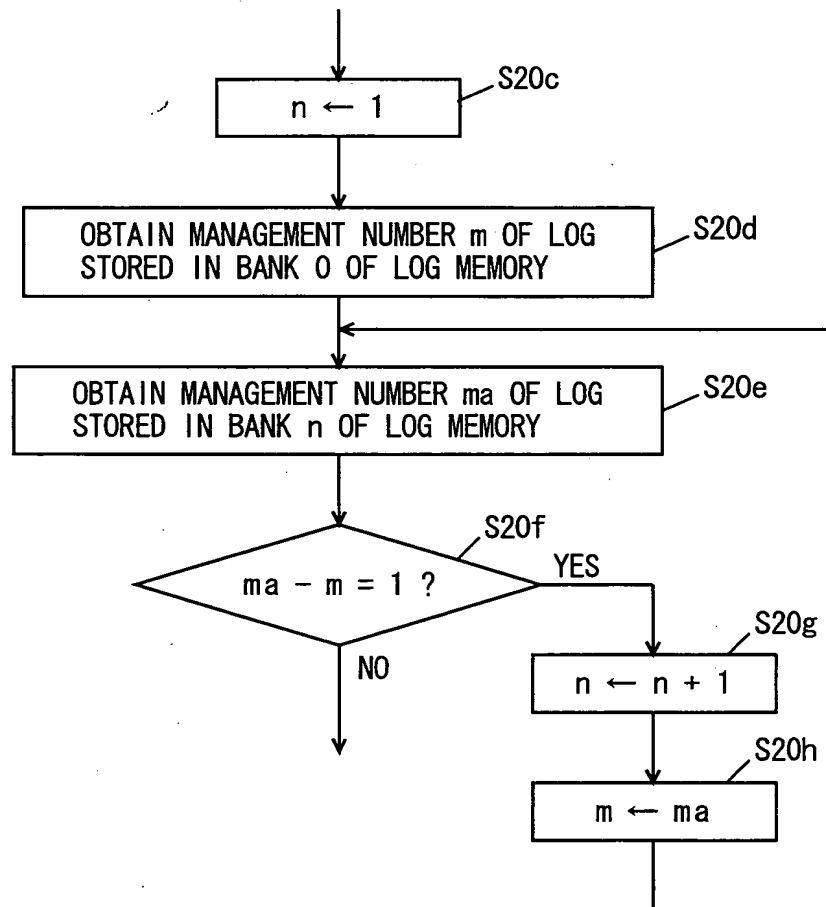


FIG. 13

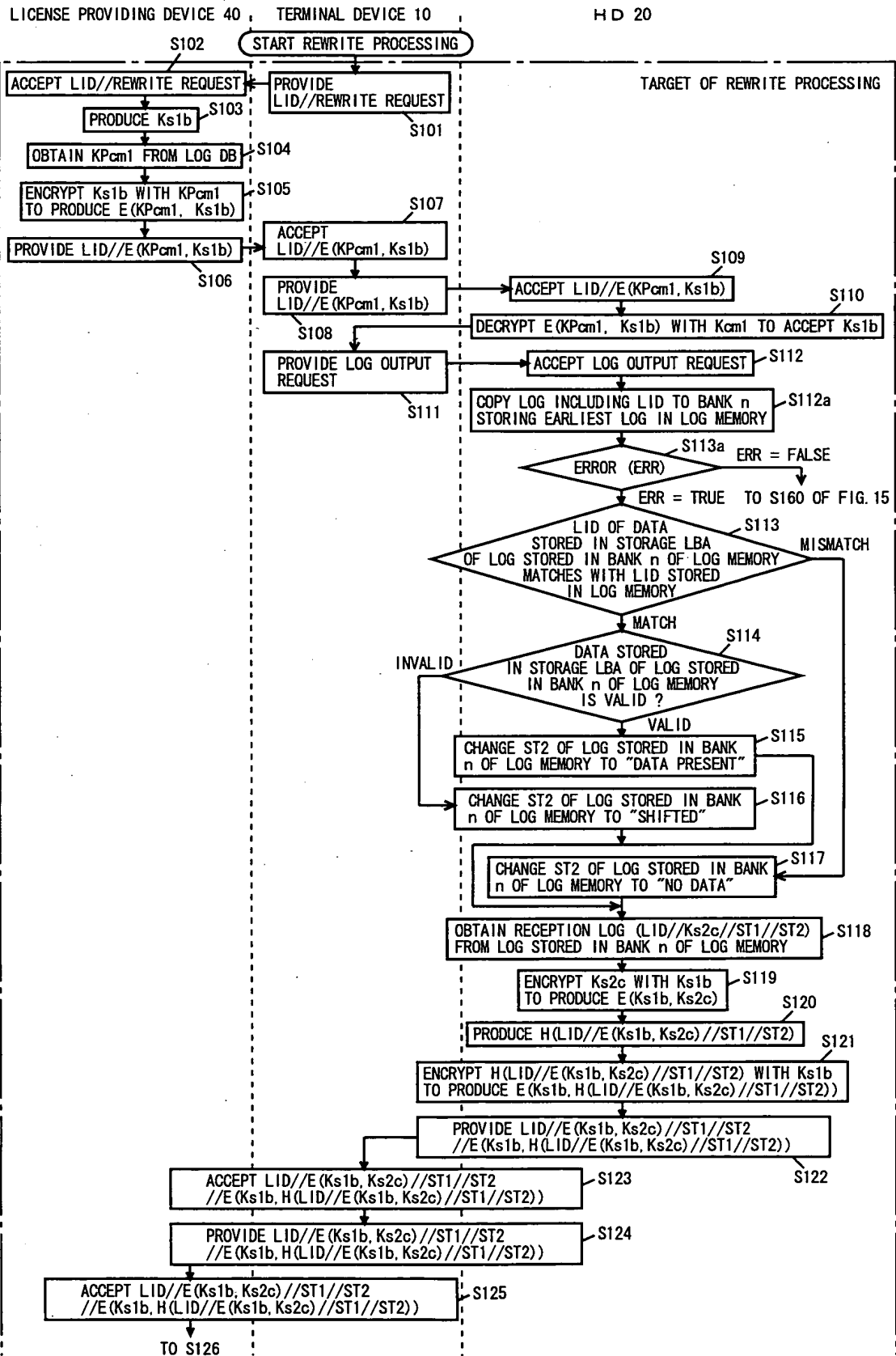


FIG. 14

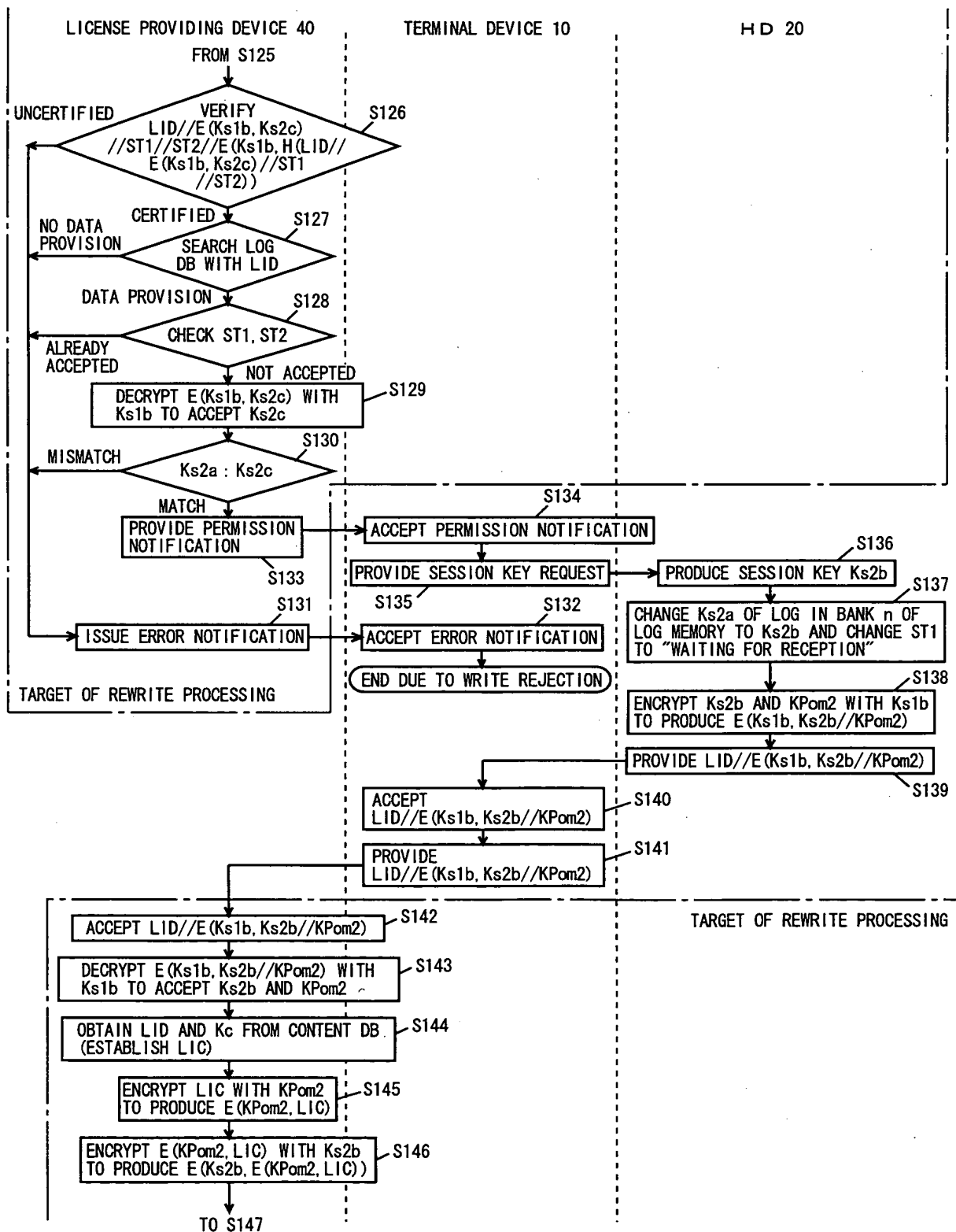


FIG. 15

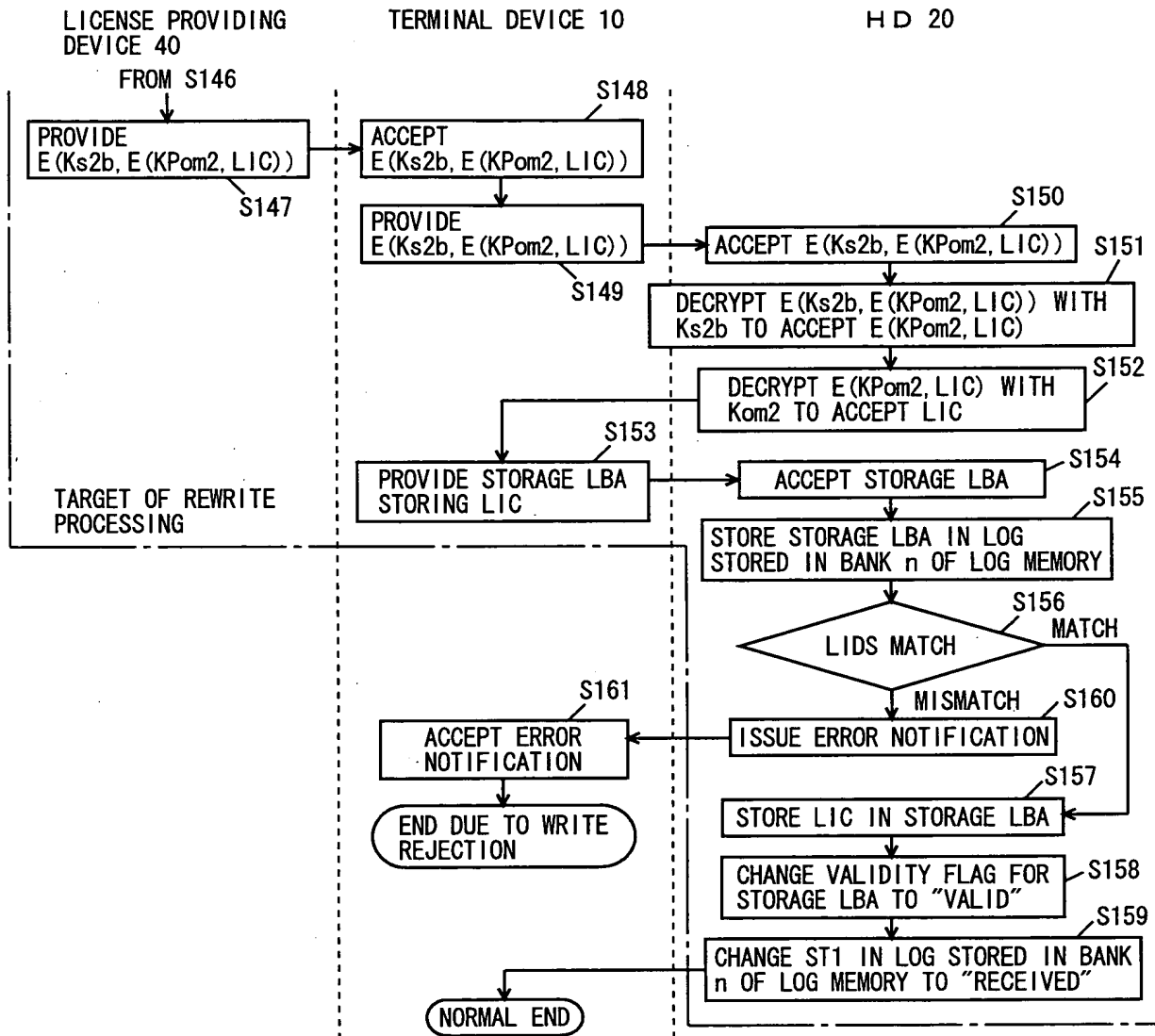


FIG. 16

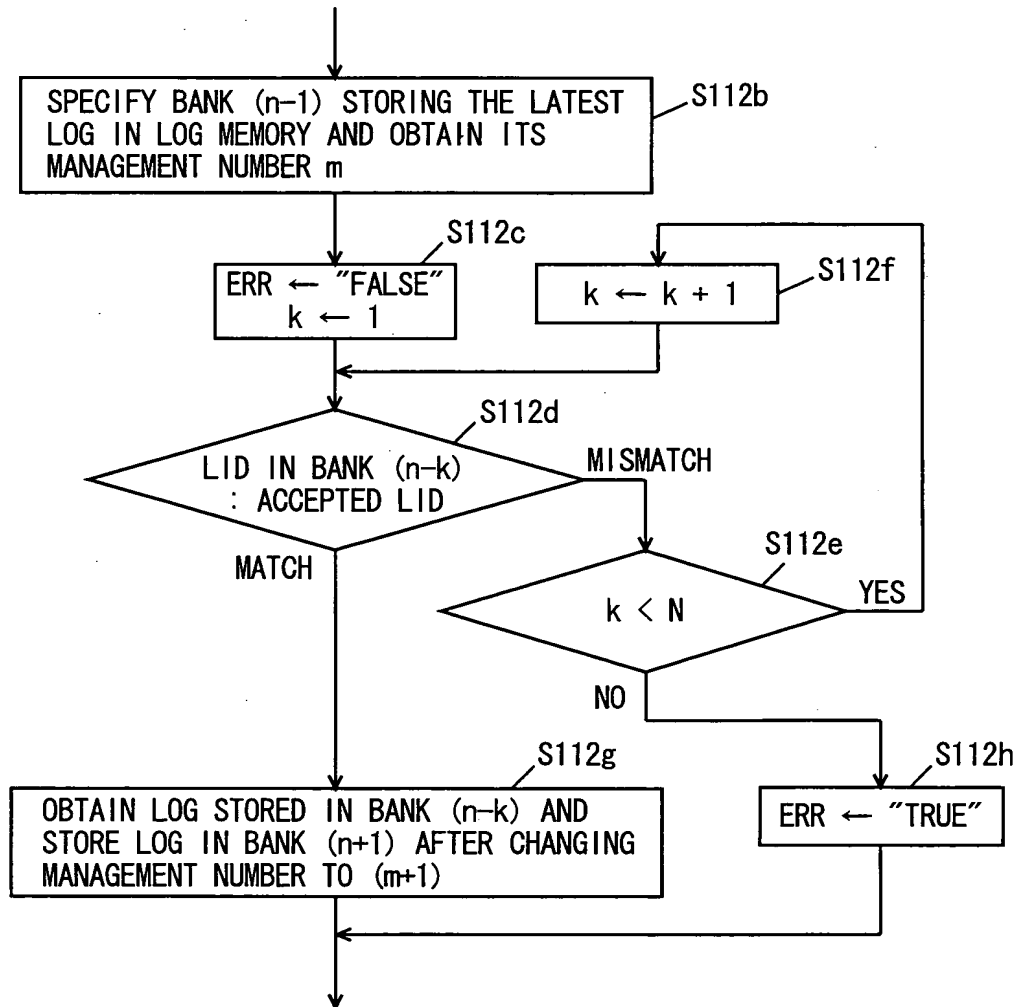
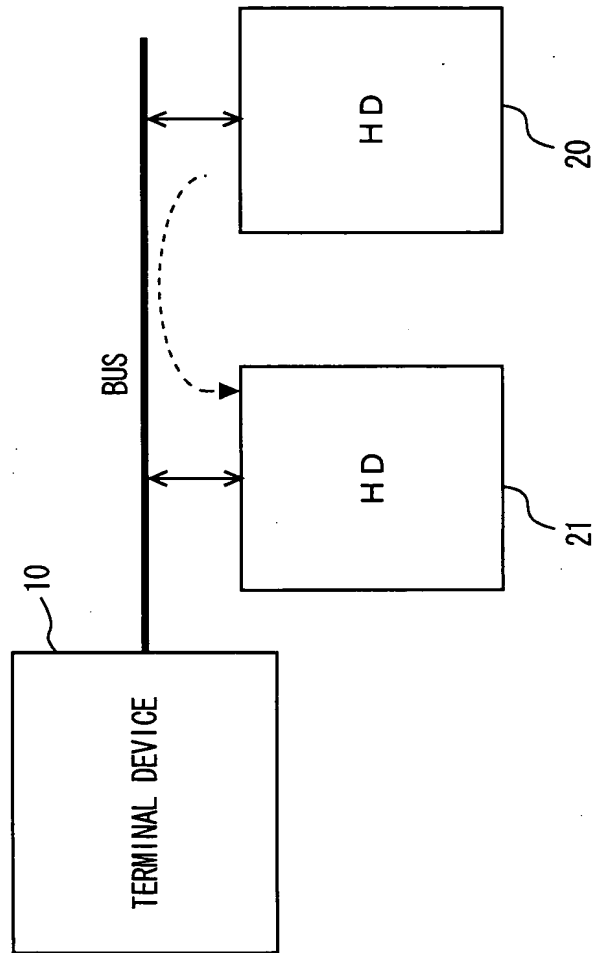
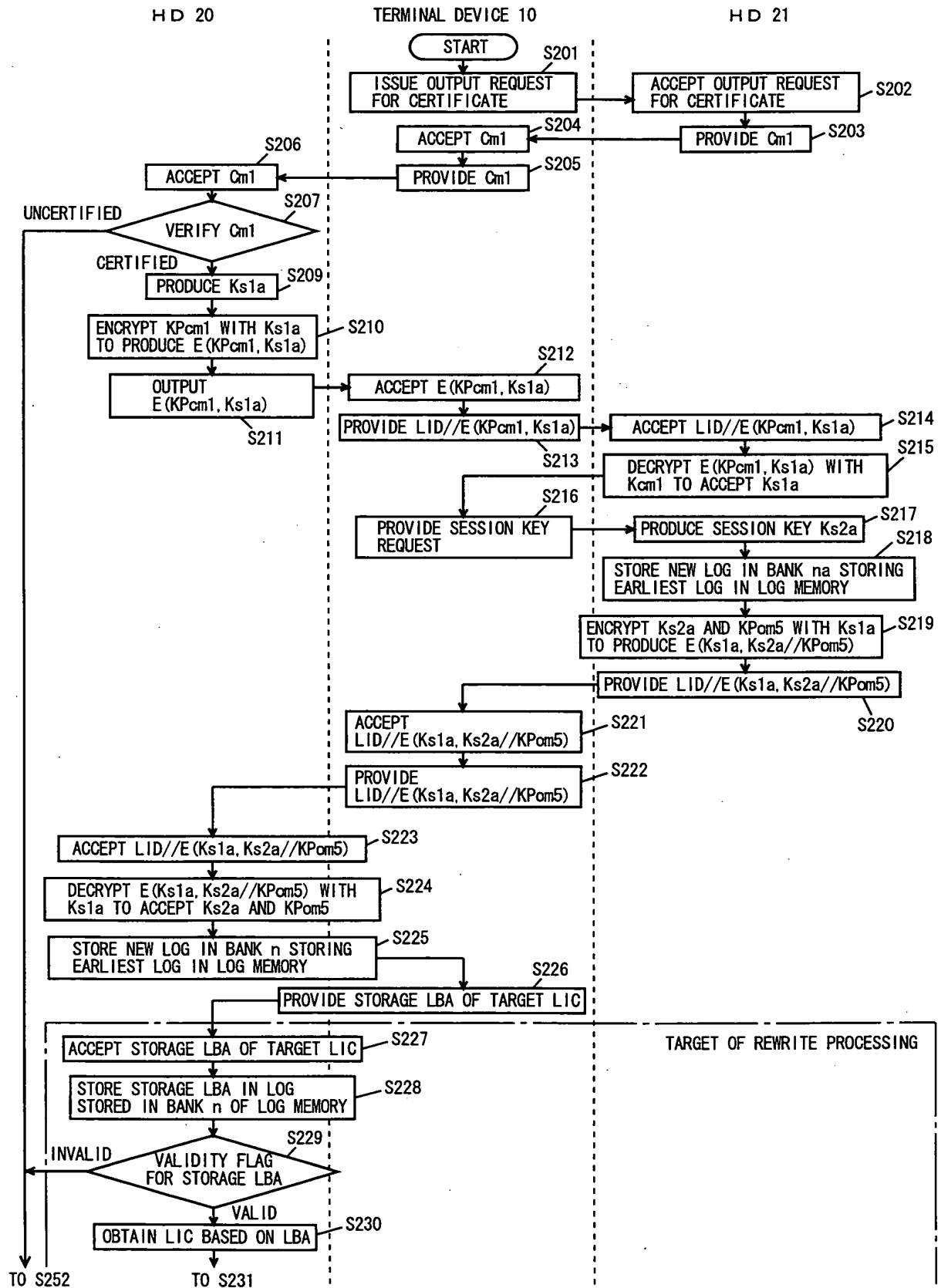


FIG. 17



HD 20



Rec'd PGT/PTO 24 JAN 2005

FIG. 19

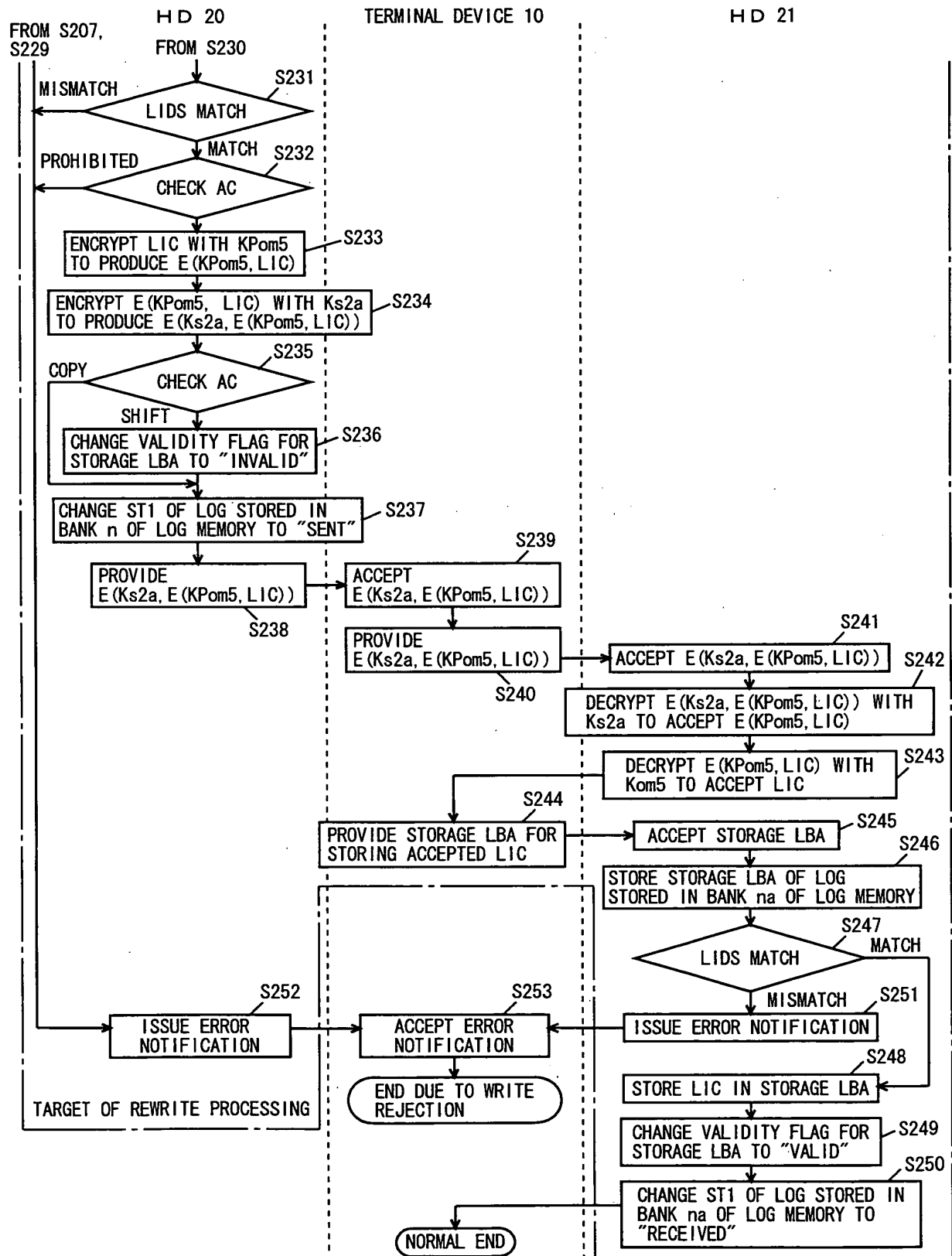


FIG. 20

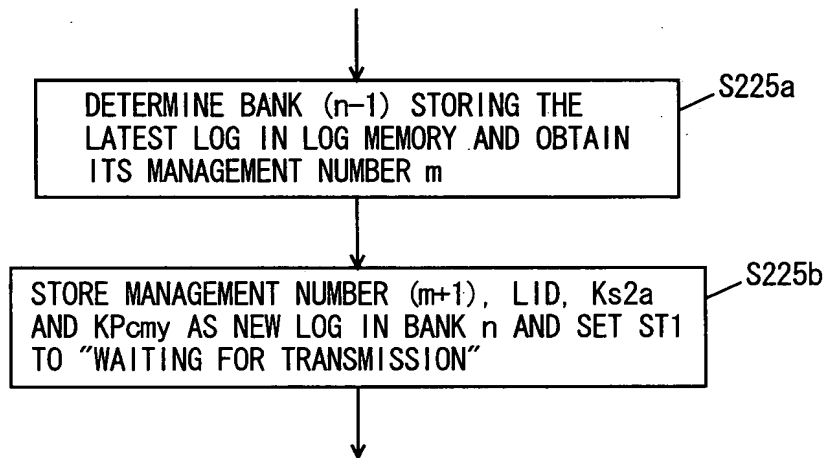
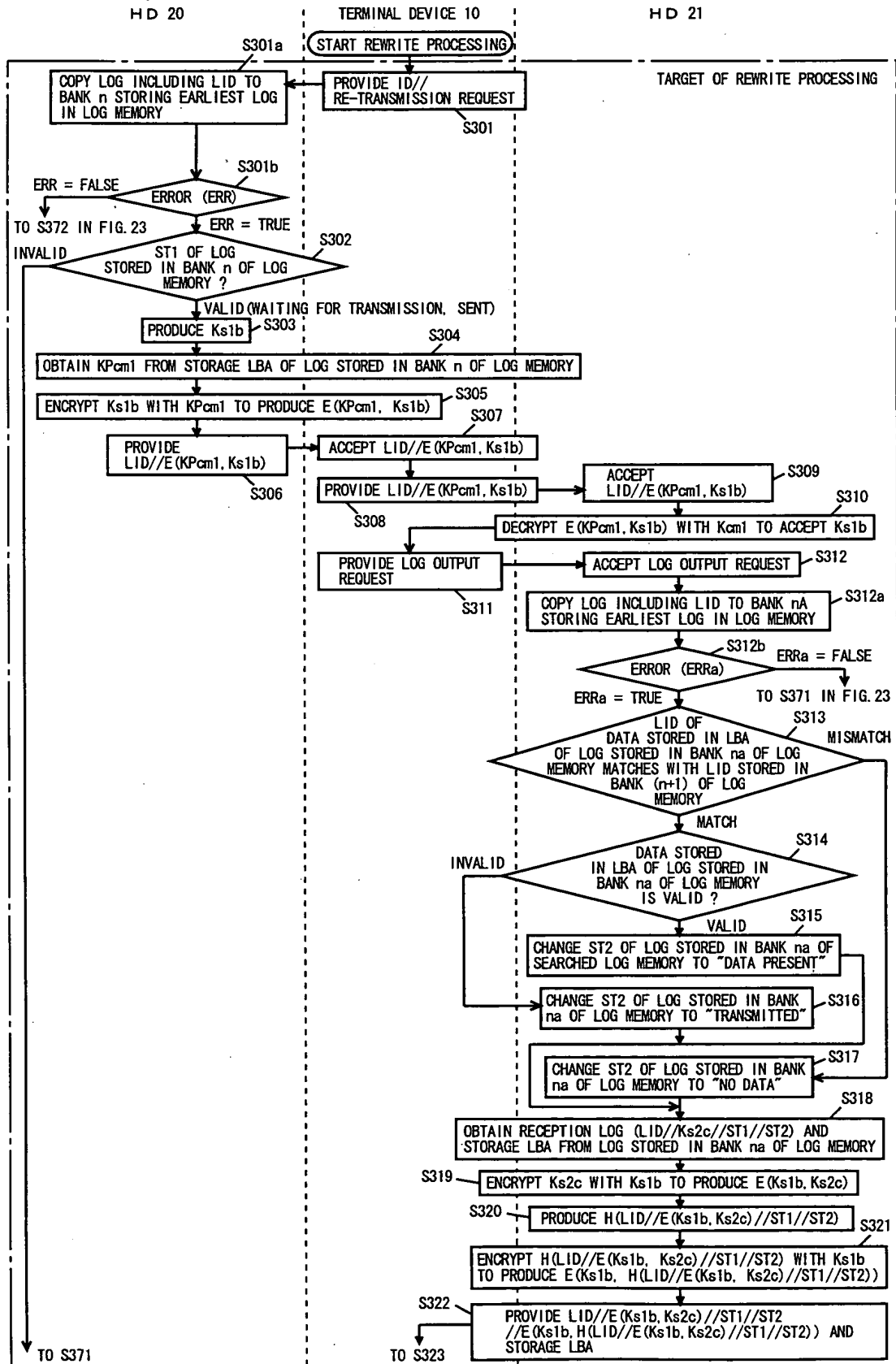
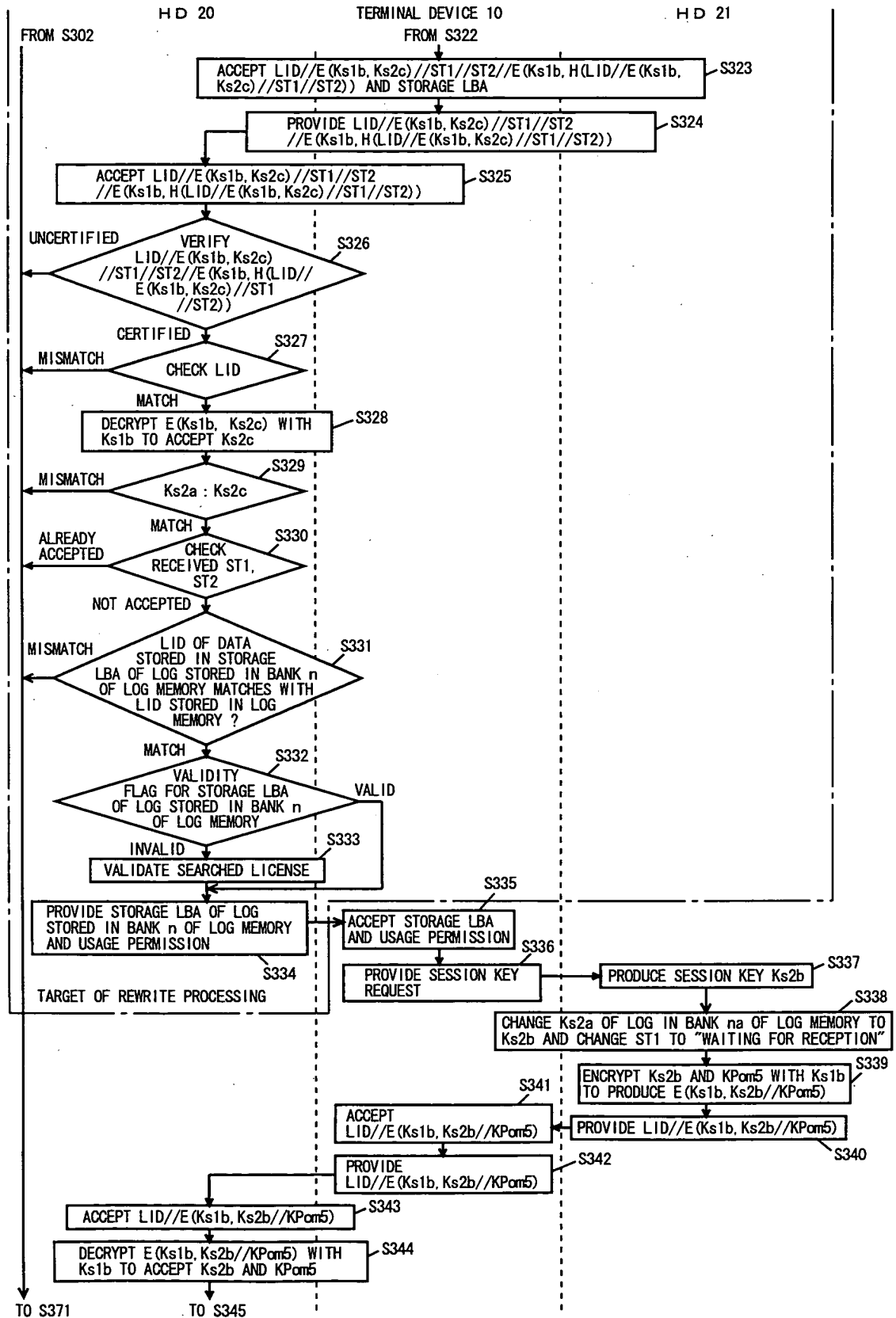


FIG. 21



Rec'd PET/PTO 24 JAN 2005

FIG. 22



Rec'd PET/PTO 24 JAN 2005

FIG. 23

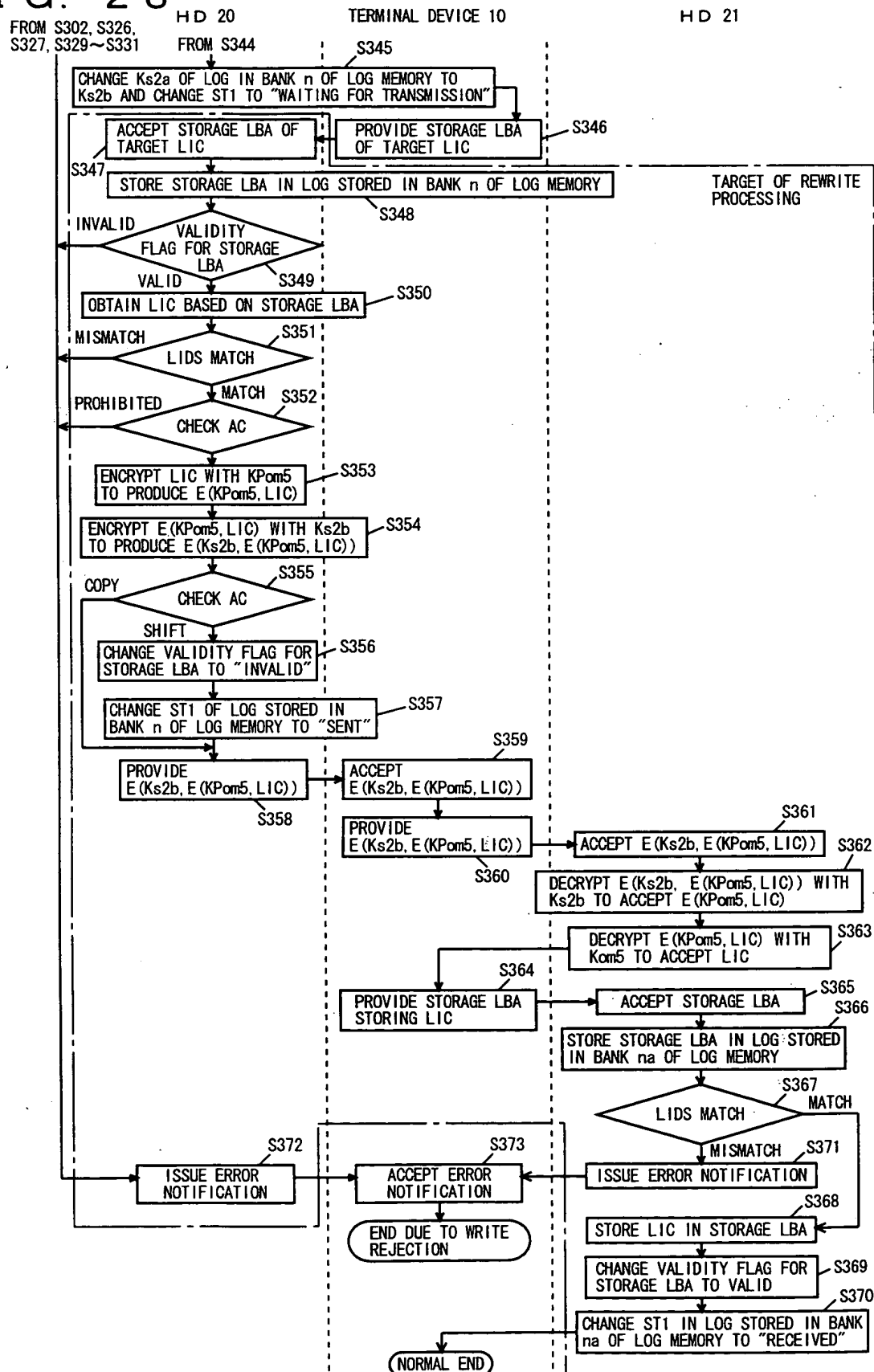


FIG. 24

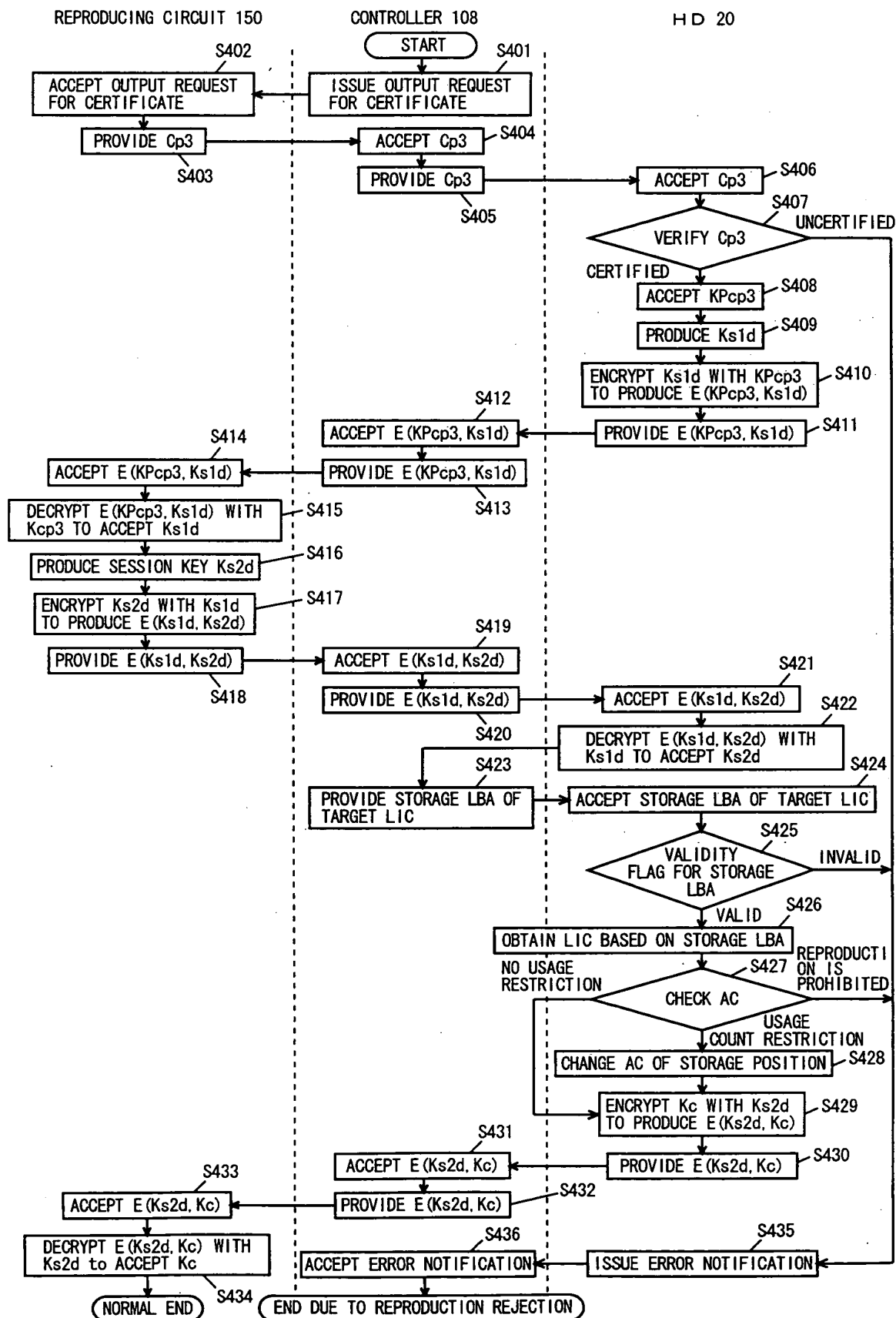


FIG. 25

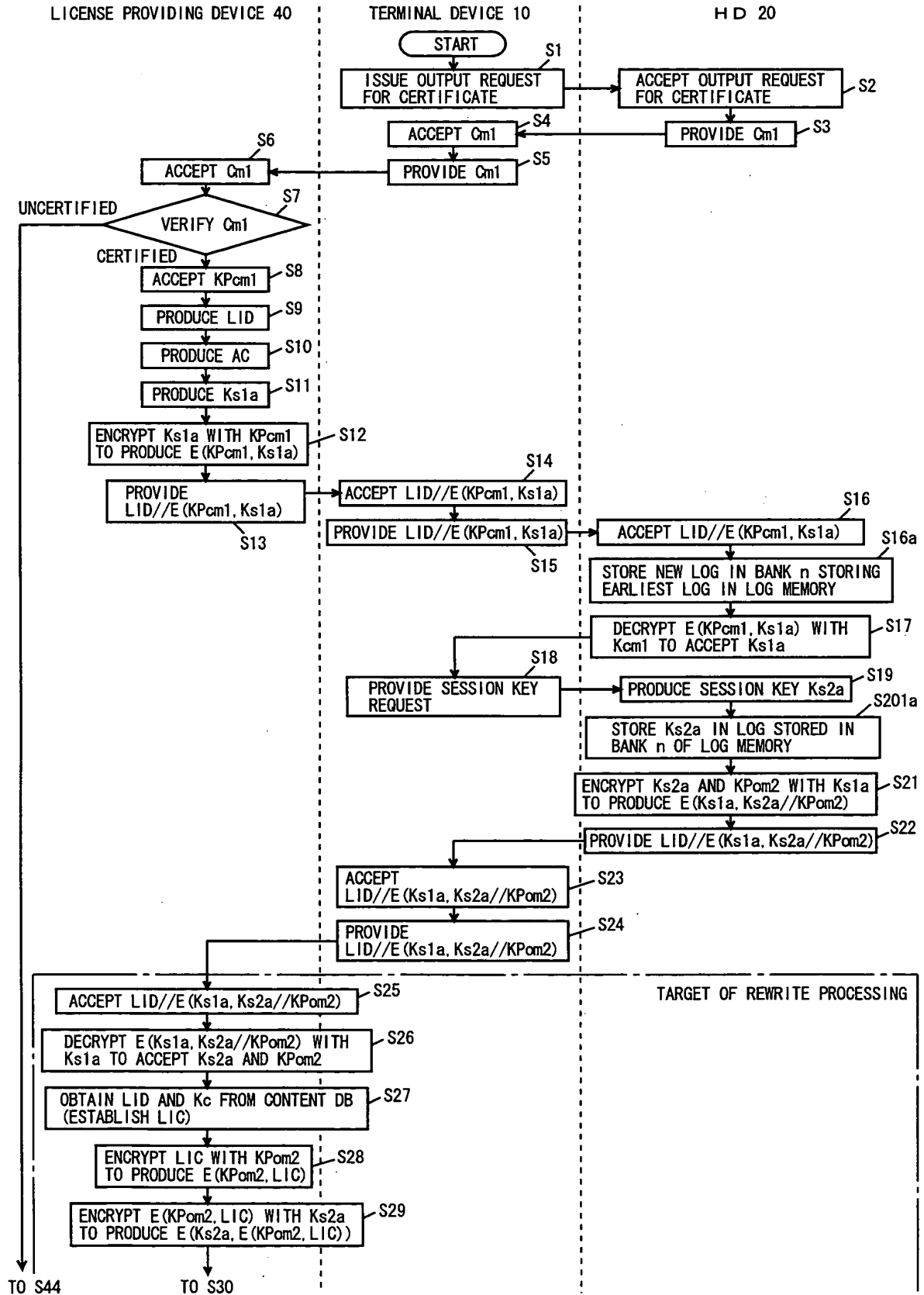


FIG. 26

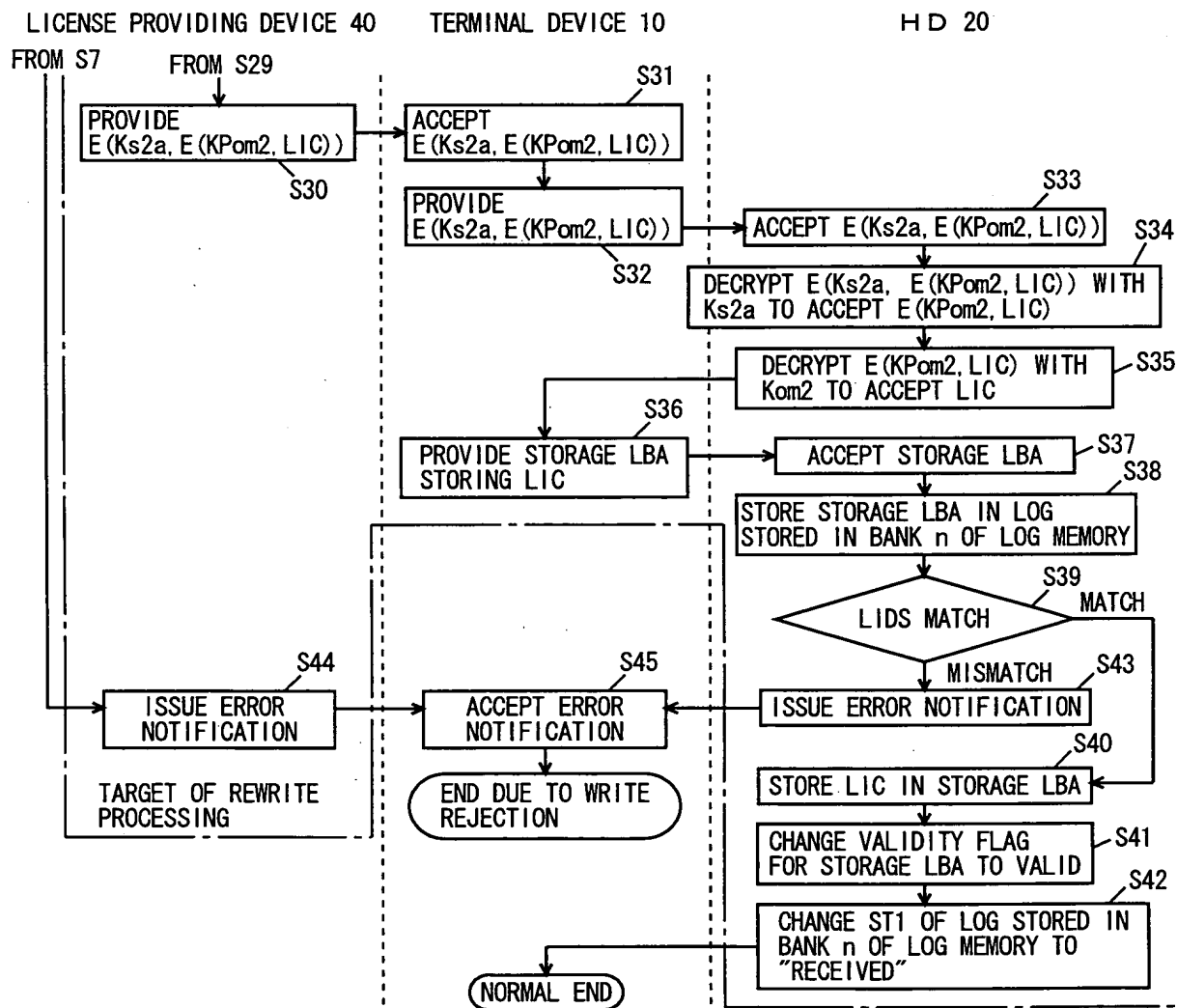
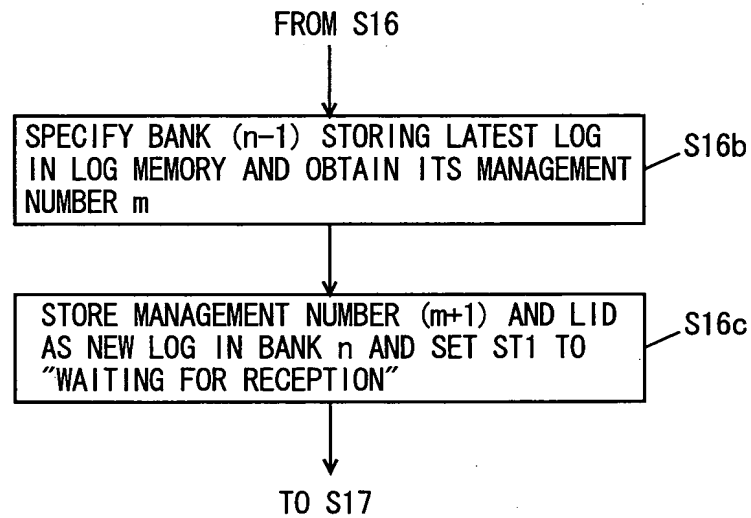
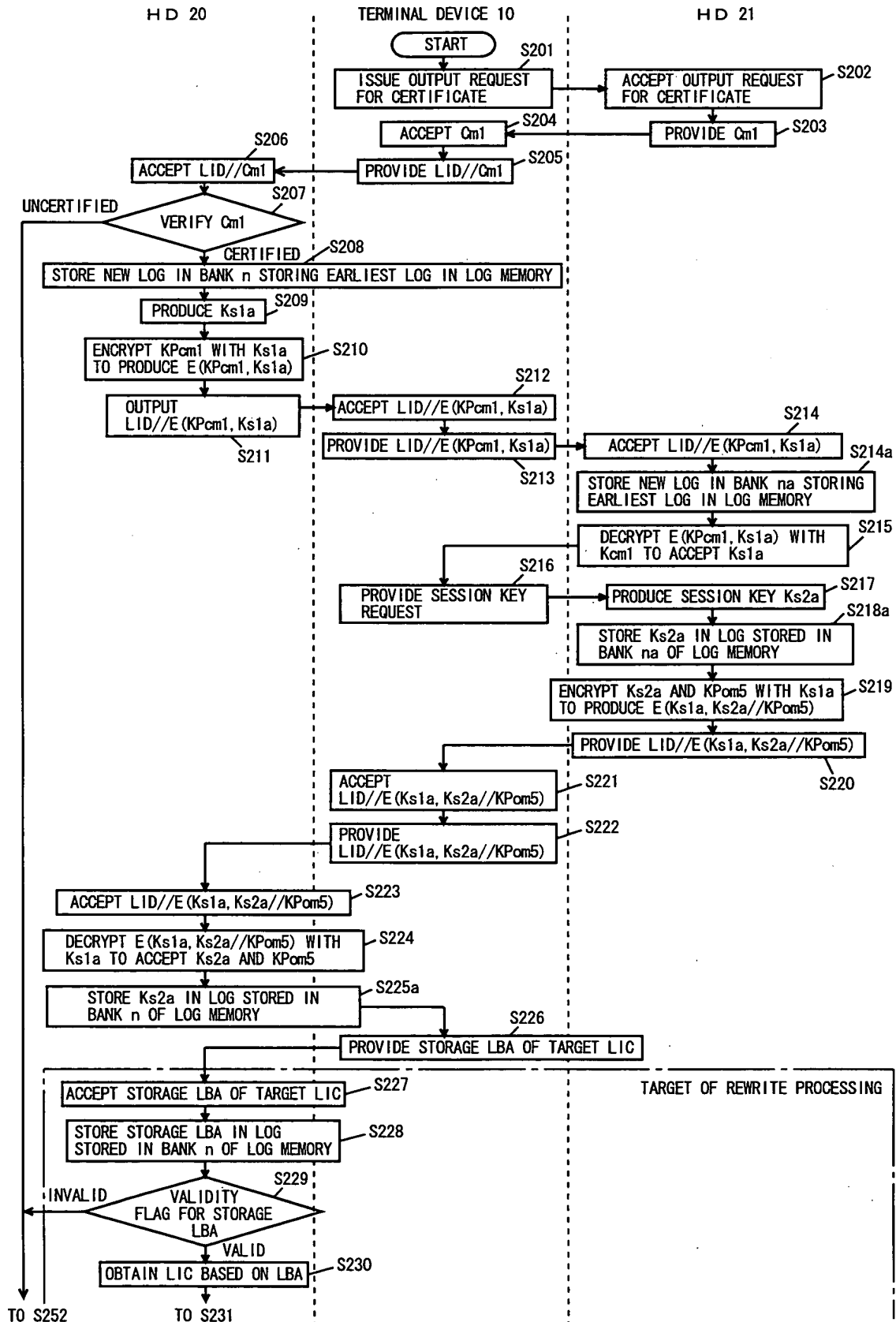


FIG. 27



Rec'd PET/PTO 24 JAN 2005

FIG. 28



```

graph TD
    subgraph "HD 20"
        S207[S207] --> S229[S229]
        S229 --> S231{S231  
LIDS MATCH}
        S231 -- MISMATCH --> S252[S252  
ISSUE ERROR NOTIFICATION]
        S231 -- MATCH --> S232{S232  
CHECK AC}
        S232 -- PROHIBITED --> S252
        S232 -- MATCH --> S233[S233  
ENCRYPT LIC WITH KPom5  
TO PRODUCE E(KPom5, LIC)]
        S233 --> S234[S234  
ENCRYPT E(KPom5, LIC) WITH Ks2a  
TO PRODUCE E(Ks2a, E(KPom5, LIC)) ]
        S234 --> S235{S235  
CHECK AC}
        S235 -- COPY --> S236[S236  
CHANGE VALIDITY FLAG FOR  
STORAGE LBA TO INVALID]
        S235 -- SHIFT --> S237[S237  
CHANGE ST1 OF LOG STORED IN  
BANK n OF LOG MEMORY TO "SENT"]
        S236 --> S237
        S237 --> S238[S238  
PROVIDE E(Ks2a, E(KPom5, LIC)) ]
        S238 --> S239[S239  
ACCEPT E(Ks2a, E(KPom5, LIC)) ]
        S239 --> S240[S240  
PROVIDE E(Ks2a, E(KPom5, LIC)) ]
        S240 --> S241[S241  
ACCEPT E(Ks2a, E(KPom5, LIC)) ]
        S241 --> S242[S242  
DECRYPT E(Ks2a, E(KPom5, LIC)) WITH  
Ks2a TO ACCEPT E(KPom5, LIC)]
        S242 --> S243[S243  
DECRYPT E(KPom5, LIC) WITH  
Kom5 TO ACCEPT LIC]
        S243 --> S244[S244  
PROVIDE STORAGE LBA FOR  
STORING ACCEPTED LIC]
        S244 --> S245[S245  
ACCEPT STORAGE LBA]
        S245 --> S246[S246  
STORE STORAGE LBA IN LOG  
STORED IN BANK na OF LOG MEMORY]
        S246 --> S247{S247  
LIDS MATCH}
        S247 -- MATCH --> S248[S248  
STORE LIC IN STORAGE LBA]
        S247 -- MISMATCH --> S251[S251  
ISSUE ERROR NOTIFICATION]
        S248 --> S249[S249  
CHANGE VALIDITY FLAG FOR  
STORAGE LBA TO VALID]
        S249 --> S250[S250  
CHANGE ST1 OF LOG STORED IN BANK  
na OF LOG MEMORY TO "RECEIVED"]
        S251 --> S252
        S250 --> S253[S253  
ACCEPT ERROR NOTIFICATION]
        S252 --> S253
        S253 --> S254([S254  
END DUE TO WRITE  
REJECTION])
        S254 --> S255([S255  
NORMAL END])
    end

    subgraph "TERMINAL DEVICE 10"
        S239 --> S238
        S240 --> S239
        S241 --> S240
        S242 --> S241
        S243 --> S242
        S244 --> S243
        S245 --> S244
        S246 --> S245
        S247 --> S246
        S248 --> S247
        S249 --> S248
        S250 --> S249
    end

    subgraph "HD 21"
        S241 --> S240
        S242 --> S241
        S243 --> S242
        S244 --> S243
        S245 --> S244
        S246 --> S245
        S247 --> S246
        S248 --> S247
        S249 --> S248
        S250 --> S249
    end

    S252 --> S253
    S253 --> S254
    S254 --> S255

```

```

graph TD
    subgraph "HD 20"
        S207[S207] --> S229[S229]
        S229 --> S231{S231  
LIDS MATCH}
        S231 -- MISMATCH --> S232{S232  
CHECK AC}
        S231 -- MATCH --> S232
        S232 -- PROHIBITED --> S233[ENCRYPT LIC WITH KPom5  
TO PRODUCE E(KPom5, LIC)]
        S232 -- MATCH --> S233
        S233 --> S234[ENCRYPT E(KPom5, LIC) WITH Ks2a  
TO PRODUCE E(Ks2a, E(KPom5, LIC))]
        S234 --> S235{S235  
CHECK AC}
        S235 -- COPY --> S236[CHANGE VALIDITY FLAG FOR  
STORAGE LBA TO INVALID]
        S235 -- SHIFT --> S236
        S236 --> S237[CHANGE ST1 OF LOG STORED IN  
BANK n OF LOG MEMORY TO "SENT"]
        S237 --> S238[PROVIDE  
E(Ks2a, E(KPom5, LIC))]
        S238 --> S239[ACCEPT  
E(Ks2a, E(KPom5, LIC))]
        S239 --> S240[PROVIDE  
E(Ks2a, E(KPom5, LIC))]
        S240 --> S241[ACCEPT E(Ks2a, E(KPom5, LIC))]
        S241 --> S242[DECRYPT E(Ks2a, E(KPom5, LIC)) WITH  
Ks2a TO ACCEPT E(KPom5, LIC)]
        S242 --> S243[DECRYPT E(KPom5, LIC) WITH  
Kom5 TO ACCEPT LIC]
        S243 --> S244[ACCEPT STORAGE LBA]
        S244 --> S245[STORE STORAGE LBA IN LOG  
STORED IN BANK na OF LOG MEMORY]
        S245 --> S246{S246  
LIDS MATCH}
        S246 -- MATCH --> S247[ISSUE ERROR NOTIFICATION]
        S246 -- MISMATCH --> S248[STORE LIC IN STORAGE LBA]
        S247 --> S249[CHANGE VALIDITY FLAG FOR  
STORAGE LBA TO VALID]
        S248 --> S249
        S249 --> S250[CHANGE ST1 OF LOG STORED IN BANK  
na OF LOG MEMORY TO "RECEIVED"]
        S250 --> S251[END]
    end

    subgraph "TERMINAL DEVICE 10"
        S231 -- MISMATCH --> S252[ISSUE ERROR NOTIFICATION]
        S232 -- PROHIBITED --> S252
        S235 -- COPY --> S252
        S235 -- SHIFT --> S252
        S237 --> S253[ACCEPT ERROR NOTIFICATION]
        S240 --> S253
        S247 --> S253
        S252 --> S253
        S253 --> S254[END DUE TO WRITE REJECTION]
    end

    S254 --> S255[NORMAL END]

```

FIG. 30

